UNITED STATES PATENT APPLICATION

FOR

A METHOD AND APPARATUS FOR MANAGING ELECTRONIC COMMERCE

Inventors:

Jean M. Goldschmidt Iki
Anthony Alexander Shah-Nazaroff

prepared by:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Blvd., 7th Floor
Los Angeles, California 90025-1026
(303) 740-1980

Attorney Docket No.: 042390.P4495C

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number EL695838561US

Date of Deposit August 4, 2000

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner of Patents and Trademarks, Washington, D. C. 20231

April M. Worley
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

A METHOD AND APPARATUS FOR MANAGING ELECTRONIC COMMERCE

FIELD OF THE INVENTION

The present invention relates to the field of electronic commerce. More specifically, the present invention relates to a method and apparatus for managing electronic commerce.

BACKGROUND OF THE INVENTION

Commerce on the Internet is attracting enormous financial interest from businesses large and small. The Internet is attractive to businesses because it enables them to reach a large audience and generate an impressive presence regardless of the size of the business. For many businesses, Internet commerce involves a business running a server system that takes credit card orders from a customer running a client system over the Internet. Sending and receiving sensitive information over the Internet raises many security issues. Some of these security issues include maintaining privacy by insuring that the information is inaccessible to anyone but the sender and receiver, and guaranteeing non-fabrication by insuring that the receiver is genuine.

Several software programs made available for client and server communication provide a Secure Socket Layer (SSL) protocol that employs a variety of standard encryption algorithms including the government and banking standard of Data Encryption Standard (DES) and several Rivest, Shamir, and Adleman (RSA) algorithms including RC4. SSL enables a client and server to exchange a secret number known as a Master_Key. After the Master_Key is shared, the client and server use the Master_Key to create a different set of keys called Session Keys. These keys are used with a specified cryptographic algorithm to encrypt and decrypt the contents of the communication session.

Even with the security measures provided through the SSL protocol in client and server software, communications between clients and servers are not unbreakable. Furthermore, regardless of how labor intensive the SSL protocol makes for an intruder to break an encrypted message between a client and server, the SSL protocol fails to provide a mechanism for insuring that the receiver is a genuine business.

SUMMARY

A method for managing electronic commerce according to a first embodiment of the present invention is disclosed. Consumer information is stored. A request made by the consumer to make a transaction and the consumer information is securely forwarded to a party in the transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not by way of limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

Figure 1 is a block diagram illustrating a network in which an embodiment of the present invention is implemented;

Figure 2 is a block diagram illustrating the system components of one embodiment of a client system according to the present invention;

Figure 3 is a block diagram illustrating one embodiment of a system controller according to the present invention;

Figure 4 is a block diagram of modules implementing an embodiment of an electronic commerce manager according to the present invention;

Figure 5 is a block diagram of modules implementing an embodiment of a transaction manager according to the present invention; and

Figure 6 is a flow chart illustrating a method for managing electronic commerce according to an embodiment of the present invention.

DETAILED DESCRIPTION

Figure 1 is a block diagram illustrating a network in which an embodiment of the present invention is implemented. Block 110 represents a client system. Block 130 represents an electronic commerce system. Block 150 represents a server system. The client system 110 and the electronic commerce system 130 are coupled to a first transmission medium 120. The electronic commerce system 130 and the server system 150 are coupled to a second transmission medium 140.

According to an embodiment of the present invention, sending data on the first transmission medium 120 is insecure because the data may be monitored and read by someone other than a sender or receiver of the data. According to one embodiment of the present invention, the transmission medium may be the Internet. When a user of the client system 110 wishes to transmit sensitive information to another location such as the server system 150, the client system 110 sends the request to the electronic commerce system 130 over the first transmission medium 120 without actually sending the sensitive information. The electronic commerce system 130 stores consumer information including sensitive information such as credit information corresponding to the user. According to one embodiment of the present invention, the electronic commerce system 130 forwards the sensitive information to the server system 150 securely over the second transmission medium 140 upon receiving the request from the client system 110. In this embodiment, the second transmission medium 140 may be a direct telephone connection. According to a second embodiment of the present invention, the electronic commerce system 130 encrypts the sensitive information and forwards the encrypted sensitive information securely over the second transmission medium 140 upon receiving a request from the client system 110. In this embodiment, the second transmission medium 140 may be the Internet.

According to an embodiment of the present invention, the electronic commerce system 130 includes an information distributor that sends transactional information to the client system 110. According to an alternate embodiment of the present invention, the server system 150 includes an information distributor that sends the transactional information to the client system 110. In this embodiment, the electronic commerce system 130 verifies that the server system 150 is genuine before forwarding the sensitive information to the server system 150 as requested by the client system 110.

Figure 2 is a block diagram illustrating system components of a client system 110 (shown in Figure 1) according to one embodiment of the present invention. According to this embodiment, the client system 110 is an entertainment system 200 that includes a common input/output (I/O) bus 210 that connects the system components in the entertainment system 200 together. It should be appreciated that the common I/O bus 210 is illustrated to simplify the routing of signals between the computer system components. The common I/O bus 210 may represent a plurality of known mechanisms and techniques for routing I/O signals between the computer system components. For example, the common I/O bus 210 may include an appropriate number of independent audio "patch" cables that route audio signals, coaxial cables that route video signals, two-wire serial lines or infrared or radio frequency transceivers that route control signals, or other routing mechanisms that route other signals.

In the illustrated embodiment, the entertainment system 200 includes a television/monitor 221, video recorder/playback device 222, digital video disk (DVD) recorder/playback device 223, audio/video tuner and amplifier 224, audio playback/recorder device 225, and compact disk player 226 coupled to the common I/O bus. The video recorder/playback device 222, DVD recorder/playback device 223, audio playback/recorder device 225, and compact disk player 226 may be single disk or

single cassette devices, or alternatively may be multiple disk or multiple cassette devices.

In addition, the entertainment system 200 includes a speaker system 231, microphone 232, video camera 233, and a wireless I/O control device 234. In one embodiment, wireless I/O control device 234 is an entertainment system remote control unit which communicates with the components of the entertainment system 200 through IR signals. In another embodiment, wireless I/O control device 234 may be a wireless keyboard and cursor positioning device that communicates with the components of entertainment system 200 through IR signals or RF signals. In yet another embodiment, wireless I/O control device 234 may be an IR remote control device similar in appearance to a typical entertainment system remote control with the added feature of a track-ball, which allows a user to position a cursor on a display of the entertainment system 200.

The entertainment system 200 also includes a system controller 240. According to one embodiment of the present invention, the system controller 240 operates to receive transactional information from either the electronic commerce system 130 or the server system 150 along with broadcast data available from the server system 150 or other broadcast data sources. The transactional information is presented to a user of the entertainment system 200 during the viewing of broadcast data. The transactional information may be used by the user, for example, to purchase a product related to the user's viewing selection. According to another embodiment of the present invention, system controller 240 is configured to control a wide variety of features associated with each of the system components. As shown in Figure 2, system controller 240 is coupled, either directly or indirectly, to each of the system components, as necessary, through I/O bus 210. In one embodiment, in addition to or in place of I/O bus 210, system controller 240 is configured with a wireless communication transmitter (or

transceiver), which is capable of communicating with the system components via IR signals or RF signals 210'. Regardless of the control medium, the system controller 240 is configured to control one or more of the entertainment system components of the entertainment system 200, although it is understood that each of the components may be individually controlled with wireless I/O control device 234.

As illustrated in Figure 2, entertainment system 200 may be configured to receive broadcast data from a wide variety of sources. In one embodiment, entertainment system 200 receives broadcast data from any or all of the following sources: cable broadcast 241, satellite broadcast 242 (e.g., via a satellite dish), very high frequency (VHF) or ultra high frequency (UHF) radio frequency communication of the broadcast networks 243 (e.g., via an aerial antenna), telephone/computer network interface 244, and/or information stored locally at system controller 240 or another component of the entertainment system 200. Further, it will be appreciated by one skilled in the art, that cable broadcast input 241, satellite broadcast input 242 and VHF/UHF input 243 may receive input from digital broadcast programming and digital cable programming. The broadcast data may be received by the entertainment system 200 via the audio/video tuner and amplifier 224, the system controller 240, or other system components or combination of system components.

Although the present invention is described in the context of the exemplary embodiments presented in the figures, those skilled in the art will appreciate that the present invention is not limited to these embodiments and may be practiced in a variety of alternate embodiments. Accordingly, the innovative features of the present invention may be practiced in a system of greater or lesser complexity than that of the system depicted in Figure 2. For example, according to one embodiment, the client system 110 may be practiced using the system controller 240 alone.

Figure 3 is a block diagram illustrating a computer system 300 that may be used to implement the electronic commerce system 130 (shown in Figure 1). The computer system 300 includes a processor 301 that processes digital data signals. The processor 301 may be a complex instruction set computer (CISC) microprocessor, a reduced instruction set computing (RISC) microprocessor, a very long instruction work (VLIW) microprocessor, a processor implementing a combination of instruction sets, or other processor device. Figure 3 shows an example of the present invention implemented on a single processor computer system 300. However, it is understood that the present invention may be implemented in a computer system having multiple processors. The processor 301 is coupled to a CPU bus 310 which transmits data signals between processor 301 and other components in the computer system 300.

As an example, memory 313 may be a dynamic random access memory (DRAM) device, a static random access memory (SRAM) device, or other memory device. The memory 313 stores information or other intermediate data signals that are executed by the processor 301. A cache memory 302 resides inside processor 301 that stores information or other intermediate data that is stored in memory 213. The cache 302 speeds up memory accesses by the processor 301 by taking advantage of its locality of access. In an alternate embodiment of the computer system 300, the cache 302 or a second cache resides external to the processor 301.

A bridge memory controller 311 is coupled to the CPU bus 310 and the memory 313. The bridge memory controller 311 directs data signals between the processor 301, the memory 313, and other components in the computer system 300 and bridges the data signals from these components to a first I/O bus 320.

The first I/O bus 320 may be a single bus or a combination of multiple buses. As an example, the first I/O bus 320 may be a high performance I/O bus that operates at high throughput rates. The first I/O bus 320 may include for example a Peripheral

Components Interconnect (PCI) bus, a Personal Computer Memory Card International Association (PCMCIA) bus, a NuBus, or other buses. The first I/O bus 320 provides communication links between components in the computer system 300. A network controller 321 links the computer system 300 to a network of computers and supports communication among the machines. A display device controller 322 is coupled to the first I/O bus 320. The display device controller 322 allows coupling of a display device to the computer system 300 and acts as an interface between the display device and the computer system 300. The display device controller may be a monochrome display adapter (MDA) card, a color graphics adapter (CGA) card, an enhanced graphics adapter (EGA) card, an extended graphics array (XGA) card or other display device controller. The display device may be a television set, a computer monitor, a flat panel display or other display device. The display device receives data signals from the processor 301 through the display device controller 322 and displays the information and data signals to the user of the computer system 300.

A second I/O bus 330 may be a single bus or a combination of multiple buses. The second I/O bus 330 may include an Industry Standard Architecture (ISA) bus, an Extended Industry Standard Architecture (EISA) bus, or other buses. The second I/O bus 330 provides communication links between components in the computer system 300. A keyboard interface 332 may be a keyboard controller or other keyboard interface. The keyboard interface 332 may be a dedicated device or can reside in another device such as a bus controller or other controller. The keyboard interface 332 allows coupling of a keyboard to the computer system 300 and transmits data signals from a keyboard to the computer system 300. A data storage device 331 may be a hard disk drive, a floppy disk drive, a CD-ROM device, a flash memory device or other mass storage device. An audio controller 333 operates to coordinate the recording and playing of sounds is also coupled to the I/O bus 330. A wireless communications

interface 334 may be an IR transceiver or a RF transceiver for transmitting and receiving signals between system components of the entertainment system 200 (shown in Figure 2).

A bus bridge 323 couples the first I/O bus 320 to the second I/O bus 330. The bus bridge 323 operates to buffer and bridge data signals between the first I/O bus 320 and the second I/O bus 330.

According to one embodiment, managing electronic commerce is performed by the computer system 300 in response to the processor 301 executing sequences of instructions contained in the memory 313. Such instructions may be read into the memory 313 from other computer-readable mediums such as data storage device 331 or from a computer connected to the network via the network controller 311. Execution of the sequences of instructions contained in the memory 313 causes the processor to manage electronic commerce, as will be described hereafter. In alternative embodiments, hard-wire circuitry may be used in place of or in combination with software instructions to implement the present invention. Thus, the present invention is not limited to any specific combination of hardware circuitry and software.

Figure 4 is a block diagram illustrating an embodiment of modules of an electronic commerce manager 400 operating in the electronic commerce system 130 (shown in Figure 1), according to the present invention. The modules may be implemented by software, hardware, or a combination of both hardware and software. The electronic commerce manager 400 includes a storage medium 410. The storage medium 410 includes a first library 411 that stores information relating to consumers. The information in the first library 410 may include names, addresses, phone numbers, credit information, identifiers, or other information corresponding to the consumers. The storage medium 410 includes a second library 412 that stores information relating to businesses that practice electronic commerce. The information in the second library

410 may include the names, physical addresses, Internet addresses, phone and fax numbers, products sold, or other information relating to the businesses. According to an embodiment of the present invention, the second library 410 stores information relating to genuine businesses practicing electronic commerce that have been verified by managers of the electronic commerce manager 400. The verification may be achieved, for example, by checking the history of the business, whether any complaints have been filed against the business, or by referencing other information relating to the business.

A transaction manager 420 is coupled to the storage medium 410. As shown in Figure 5, the transaction manager 420 includes a client interface 510, a transaction processor 520, a storage medium interface 530, and a server interface 540. The client interface 510 operates to receive a request to make a transaction from a client system 110 (shown in Figure 1). The request may include an identifier (consumer identifier) corresponding to the user of the client system 110 who is a consumer, and a transaction identifier that identifies a business and a product sold by the business. The client interface 510 forwards the request to the transaction processor 520 coupled to the client interface 510.

The transaction processor 520 obtains information about the consumer making the request via the storage medium interface 530. The transaction processor 520 references the identifier received by the client system 110 (consumer identifier) with information in the first library 411 (shown in Figure 4). The transaction processor 520 also verifies that the business the user wishes to engage in the transaction with is a genuine business via the storage medium interface 530. The transaction processor 520 references the transaction identifier received by the client system 110 with the information in the second library 412 (shown in Figure 4). The transaction processor

520 forwards the information about the consumer and the transaction identifier to the server interface 540 coupled to the transaction processor 520.

The server interface 540 operates to securely forward the request to make a transaction and the information about the consumer to the server system 150 (shown in Figure 1). According to one embodiment of the present invention, the server interface 540 is a telephone interface that operates to dial a direct telephone connection to the server system 150. A direct telephone connection provides a secure communication link where the risk of monitoring and reading of data traffic is reduced. According to a second embodiment of the present invention, the server interface 540 is an encryption unit and a network interface. The encryption unit encrypts the request and the information about the consumer before sending the request and the information over an Internet connection via the network interface. Encrypting the request and information reduces the chance that the request and information may be read by someone other than the sender or receiver. The present invention allows encryption to be performed on sensitive information and transmitted over the Internet without requiring a client system 110 to be configured with the necessary encryption hardware or software. The server interface 540 may securely forward the request to make a transaction and the information about the consumer to the server system 150 in real-time as the server interface 540 receives each request and information. In an alternate embodiment of the present invention, the server interface 540 may securely forward a plurality of requests and information using batch processing at a later time.

Referring back to Figure 4, an information distributor 430 is coupled to the transaction manager 420. The information distributor 430 operates to distribute transactional information to the client system 110 (shown in Figure 1). The transactional information may be, for example, information about a product or service that is for sale or other information. According to a first embodiment of the present

invention, the information distributor 430 may be a network interface or a telephone interface that sends transactional information to the client system 110 over the Internet or over a direct phone connection. According to a second embodiment of the present invention where the electronic commerce system 130 is used for broadcasting broadcast data, the information distributor 430 may be a vertical blanking interval encoder, a cable link encoder, or a satellite link encoder that transmits transactional information over vertical blanking intervals, available cable bandwidth, or available satellite bandwidth during the transmission of broadcast data.

Figure 6 is a flow chart that illustrates a method for managing electronic commerce according to an embodiment of the present invention. At step 601, user information and business information is stored. According to an embodiment of the present invention, consumer information is stored in a first library of a storage medium. The user information may include name, address, credit information, and an identifier corresponding to a consumer (consumer identifier). According to an embodiment of the present invention, business information is stored in a second library in the storage medium. The business information may include name, physical and Internet addresses, and product information corresponding to the business.

At step 602, transactional information is sent to the user. The transactional information may be, for example, information about a product that is for sale. According to an embodiment of the present invention, the transactional information is sent over the Internet to a user on a client system. It should be appreciated that the transactional information may be sent to the consumer via a direct phone connection, vertical blanking intervals of broadcast data, or via other communication mediums. According to an embodiment of the present invention, the transactional information is displayed to the consumer during the viewing of broadcast data by the user on a client system.

At step 603, a request to make a transaction is received from the consumer. According to an embodiment of the present invention, the user sends an identifier that identifies the consumer (consumer identifier) and a transaction identifier that identifies the transaction and a party of the transaction. According to an embodiment of the present invention, the identifier and the transaction identifier is sent by the consumer over the Internet.

At step 604, it is determined whether the party of the transaction is a genuine business. According to an embodiment of the present invention, the determination is made by referencing information in the second library of the storage medium that indicates whether the intended party of the transaction is a genuine business. If the party is a genuine business, control proceeds to step 606. If the party is not a genuine business, control proceeds to step 605.

At step 605, the request to make the transaction is terminated. According to an embodiment of the present invention, a message is sent to the user at the client system informing the consumer that the party is not a genuine business.

At step 606, the request made by the consumer to make a transaction and the consumer information corresponding to the consumer is securely forwarded to the party of the transaction. The request made by the user to make the transaction may be a request to purchase the product and the consumer information may be credit information belonging to the consumer. According to an embodiment of the present invention, the request and the consumer information is securely forwarded by transmitting the request and the consumer information over a direct phone connection. According to an alternate embodiment of the present invention, the request and the consumer information is encrypted and transmitted over the Internet.

In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however be evident that various

modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.